Farfalline
Security Assessment

Technical Report

Prepared for: Istituto Farfallino
Performed by: Alessandro Molari, Giacomo Mantani

Date: 8 Feb 2018

Contents

Introduction

The following document was written as a reference for the security assessment done by Alessandro Molari, Giacomo Mantani towards Istituto Farfallino on 8 Feb 2018.

Assets involved

The following assets were involved during the testing activities:

- **www.farfalline.it**: Main website
- **www.join.farfalline.it**: Meeting section of the website

Context & Scope

This audit has been carried out at the request of Istituto Farfallino. Its goal was to evaluate the security of the assets under test, as described in section: Assets involved.

The study focuses on main **Web Vulnerabilities** as described in **OWASP Web Application Penetration Testing Methodology**.

In particular the following testing areas have been considered:

- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Error Handling Testing
- Cryptography Testing
- Business Logic Testing
- Client Side Testing

Strength of Test

The tests were executed in Safe Check. Doing so there is no possibilities to disrupt the services during the vulnerability scans. However, this safer approach entails some risk and a lower level of strength: not all exploit were tested nor DoS or DDoS attacks were performed. Instead, external attackers would try to break into the system without having to worry about what can be damaged.

Approach

The team has done a **Black-Box Vulnerability Assessment** and **Penetration Test**. No prior knowledge of a company network is known except the endpoints mentioned above. In essence an example of this is when an external web based test is to be carried out and only the details of a website URL or IP address is supplied to the testing team. It would be their role to attempt to break into the company website or network. This would equate to an external attack carried out by a malicious hacker.

Threat

A threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. In this particular scenario we try to anticipate and overcome problems from malicious agents (both human and software) intentional or unintentional.

Information Gathering

Passive Intelligence

This section will provide information gathered through Passive Intelligence.

Passive Intelligence is intelligence gathered from indirect analysis infrastructure related information, *without* sending any traffic directly to the assets.

DNS information

- **www.farfalline.it**:

```
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24615
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.farfalline.it.           IN      A

;; ANSWER SECTION:
www.farfalline.it.    10233   IN      A       1.3.4.5

;; Query time: 34 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; MSG SIZE  rcvd: 64
```

- **www.join.farfalline.it**:

```
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1481
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
```

```
;www.join.farfalline.it.       IN      A

;; ANSWER SECTION:
www.join.farfalline.it.    10233   IN      A       1.2.3.4

;; Query time: 74 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; MSG SIZE  rcvd: 68
```

Active Intelligence

This section will show the methods and results of tasks such as infrastructure mapping, port scanning, and architecture assessment and other foot printing activities.

Active Intelligence focus on the techniques used to profile the technology in the *client* environment by sending traffic *directly* to the assets.

Nmap is the free and open source utility used for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

- **1.3.4.5**:

```
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up (0.034s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
53/tcp  open  tcpwrapped
443/tcp open  ssl/https  gws
Warning: OSScan results may be unreliable because we could not find at
↪  least 1 open and 1 closed port
Device type: general purpose|printer|specialized
Running (JUST GUESSING): OpenBSD 4.X (91%), HP embedded (86%), Crestron
↪  2-Series (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.3 cpe:/o:crestron:2_series
Aggressive OS guesses: OpenBSD 4.3 (91%), HP PSC 2400-series Photosmart
↪  printer (86%), Crestron XPanel control system (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 7 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   4.80 ms  10.20.4.254
2   29.08 ms eolo-gw.net.ngi.it (81.174.0.21)
3   38.75 ms 10.221.16.1
4   38.75 ms 72.14.222.192
5   ...
6   39.53 ms 108.170.233.143
7   38.74 ms google-public-dns-a.google.com (8.8.8.8)
```

```
OS and Service detection performed. Please report any incorrect results at
↪  https://nmap.org/submit/ .
```

- **1.2.3.4**:

```
Nmap scan report for google-public-dns-b.google.com (8.8.4.4)
Host is up (0.038s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
53/tcp  open  tcpwrapped
443/tcp open  ssl/https  gws
Warning: OSScan results may be unreliable because we could not find at
↪  least 1 open and 1 closed port
Device type: general purpose|printer|specialized
Running (JUST GUESSING): OpenBSD 4.X (91%), HP embedded (86%), Crestron
↪  2-Series (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.3 cpe:/o:crestron:2_series
Aggressive OS guesses: OpenBSD 4.3 (91%), HP PSC 2400-series Photosmart
↪  printer (86%), Crestron XPanel control system (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 7 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   2.43 ms  10.20.4.254
2   13.04 ms eolo-gw.net.ngi.it (81.174.0.21)
3   20.32 ms 10.221.16.1
4   29.90 ms 72.14.222.192
5   ...
6   23.23 ms 108.170.233.133
7   19.12 ms google-public-dns-b.google.com (8.8.4.4)

OS and Service detection performed. Please report any incorrect results at
↪  https://nmap.org/submit/ .
```

Corporate Intelligence

Personnel Intelligence

Vulnerability Assessment

Methodology

- **Reconnaissance:** The tester would attempt to gather as much information as possible about the selected network. Reconnaissance can take two forms i.e. active and passive. A passive attack is always the best starting point as this would normally defeat intrusion detection systems and other forms of protection etc. afforded to the network. This would usually involve trying to discover publicly available information by utilizing a web browser and visiting newsgroups etc. An active form would be more intrusive and may show up in audit logs and may take the form of an attempted DNS zone transfer or a social engineering type of attack.

- **Enumeration:** The tester would use varied operating system fingerprinting tools to determine what hosts are alive on the network and more importantly what services and operating systems they are running. Research into these services would then be carried out to tailor the test to the discovered services.

- **Scanning:** By use of vulnerability scanners all discovered hosts would be tested for vulnerabilities. The result would then be analysed to determine if there any vulnerabilities that could be exploited to gain access to a target host on a network.

Vulnerability Metrics

The **Common Vulnerability Scoring System** (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores.

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics.

These metric groups are described as follows:

- **Base:** Represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments

- **Temporal:** Represents the characteristics of a vulnerability that change over time but not among user environments

- **Environmental:** Represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

CVSS v3.0 Ratings

Severity	Base Score Range
Low	0.0 – 3.9
Medium	4.0 – 6.9
High	7.0 – 10.0

Metric Groups

Base Metrics

The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how a vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability. For example, a vulnerability could cause a partial loss of integrity and availability, but no loss of confidentiality.

Access Vector (AV) This metric reflects how the vulnerability is exploited. The possible values for this metric are listed below. The more remote an attacker can be to attack a host, the greater the vulnerability score.

- **Local (L)**: A vulnerability exploitable with only local access requires the attacker to have either physical access to the vulnerable system or a local (shell) account. Examples of locally exploitable vulnerabilities are peripheral attacks such as Firewire/USB DMA attacks, and local privilege escalations (e.g. sudo)

- **Adjacent Network (A)**: A vulnerability exploitable with adjacent network access requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. Examples of local networks include local IP subnet, Bluetooth, IEEE 802.11, and local Ethernet segment

- **Network (N)**: A vulnerability exploitable with network access means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable". An example of a network attack is an RPC buffer overflow

Access Complexity (AC) This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. For example, consider a buffer overflow in an Internet service: once the target system is located, the attacker can launch an exploit at will.

Other vulnerabilities, however, may require additional steps in order to be exploited. For example, a vulnerability in an email client is only exploited after the user downloads and opens a tainted attachment. The lower the required complexity, the higher the vulnerability score.

- **High (H)** Specialized access conditions exist. For example:
  - In most configurations, the attacking party must already have elevated privileges or spoof additional systems in addition to the attacking system (e.g., DNS hijacking).
  - The attack depends on social engineering methods that would be easily detected by knowledgeable people. For example, the victim must perform several suspicious or atypical actions.
  - The vulnerable configuration is seen very rarely in practice.
  - If a race condition exists, the window is very narrow.
- **Medium (M)** The access conditions are somewhat specialized; the following are examples:
  - The attacking party is limited to a group of systems or users at some level of authorization, possibly untrusted.
  - Some information must be gathered before a successful attack can be launched.
  - The affected configuration is non-default, and is not commonly configured (e.g., a vulnerability present when a server performs user account authentication via a specific scheme, but not present for another authentication scheme).
  - The attack requires a small amount of social engineering that might occasionally fool cautious users (e.g., phishing attacks that modify a web browsers status bar to show a false link, having to be on someones buddy list before sending an IM exploit).
- **Low (L)** Specialized access conditions or extenuating circumstances do not exist. The following are examples:
  - The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted (e.g., Internet-facing web or mail server).
  - The affected configuration is default or ubiquitous.
  - The attack can be performed manually and requires little skill or additional information gathering.
  - The race condition is a lazy one (i.e., it is technically a race but easily winnable).

This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability. This metric does not gauge the strength or complexity of the authentication process, only that an attacker is required to provide credentials before an exploit may occur. The fewer authentication instances that are required, the higher the vulnerability score.

- **Multiple (M)** Exploiting the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time. An example is an attacker authenticating to an operating system in addition to providing credentials to access an application hosted on that system.

- **Single (S)** The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).
- **None (N)** Authentication is not required to exploit the vulnerability.

The metric should be applied based on the authentication the attacker requires before launching an attack. For example, if a mail server is vulnerable to a command that can be issued before a user authenticates, the metric should be scored as "None" because the attacker can launch the exploit before credentials are required. If the vulnerable command is only available after successful authentication, then the vulnerability should be scored as "Single" or "Multiple," depending on how many instances of authentication must occur before issuing the command.

Confidentiality Impact (C) This metric measures the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. Increased confidentiality impact increases the vulnerability score.

- **None (N)** There is no impact to the confidentiality of the system
- **Partial (P)** There is considerable informational disclosure. Access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. An example is a vulnerability that divulges only certain tables in a database
- **Complete (C)** There is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc)

Integrity Impact (I) This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information. Increased integrity impact increases the vulnerability score.

- **None (N)** There is no impact to the integrity of the system.
- **Partial (P)** Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. For example, system or application files may be overwritten or modified, but either the attacker has no control over which files are affected or the attacker can modify files within only a limited context or scope.
- **Complete (C)** There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

Availability Impact (A) This metric measures the impact to availability of a successfully exploited vulnerability. Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of a system. Increased availability impact increases the vulnerability score.

- **None (N)** There is no impact to the availability of the system.
- **Partial (P)** There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to an Internet service.

- **Complete (C)** There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.

Temporal Metrics

The threat posed by a vulnerability may change over time. Three such factors that CVSS captures are: confirmation of the technical details of a vulnerability, the remediation status of the vulnerability, and the availability of exploit code or techniques. Since temporal metrics are optional they each include a metric value that has no effect on the score. This value is used when the user feels the particular metric does not apply and wishes to "skip over" it.

Exploitability (E)

This metric measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability.

Initially, real-world exploitation may only be theoretical. Publication of proof of concept code, functional exploit code, or sufficient technical details necessary to exploit the vulnerability may follow. Furthermore, the exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently. In severe cases, it may be delivered as the payload of a network-based worm or virus. The more easily a vulnerability can be exploited, the higher the vulnerability score.

- **Unproven (U)** No exploit code is available, or an exploit is entirely theoretical.
- **Proof-of-Concept (POC)** Proof-of-concept exploit code or an attack demonstration that is not practical for most systems is available. The code or technique is not functional in all situations and may require substantial modification by a skilled attacker.
- **Functional (F)** Functional exploit code is available. The code works in most situations where the vulnerability exists.
- **High (H)** Either the vulnerability is exploitable by functional mobile autonomous code, or no exploit is required (manual trigger) and details are widely available. The code works in every situation, or is actively being delivered via a mobile autonomous agent (such as a worm or virus).
- **Not Defined (ND)** Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Remediation Level (RL)

The remediation level of a vulnerability is an important factor for prioritization. The typical vulnerability is unpatched when initially published. Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued. Each of these respective stages adjusts the temporal score downwards, reflecting the decreasing urgency as remediation becomes final.The less official and permanent a fix, the higher the vulnerability score is.

- **Official Fix (OF)** A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available.
- **Temporary Fix (TF)** There is an official but temporary fix available. This includes instances where the vendor issues a temporary hotfix, tool, or workaround.

- **Workaround (W)** There is an unofficial, non-vendor solution available. In some cases, users of the affected technology will create a patch of their own or provide steps to work around or otherwise mitigate the vulnerability.
- **Unavailable (U There)** is either no solution available or it is impossible to apply.
- **Not Defined (ND)** Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Report Confidence (RC)

This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. Sometimes, only the existence of vulnerabilities are publicized, but without specific details. The vulnerability may later be corroborated and then confirmed through acknowledgement by the author or vendor of the affected technology. The urgency of a vulnerability is higher when a vulnerability is known to exist with certainty. This metric also suggests the level of technical knowledge available to would-be attackers. The possible values for this metric are listed below. The more a vulnerability is validated by the vendor or other reputable sources, the higher the score.

- **Unconfirmed (UC)** There is a single unconfirmed source or possibly multiple conflicting reports. There is little confidence in the validity of the reports. An example is a rumor that surfaces from the hacker underground.
- **Uncorroborated (UR)** There are multiple non-official sources, possibly including independent security companies or research organizations. At this point there may be conflicting technical details or some other lingering ambiguity.
- **Confirmed (C)** The vulnerability has been acknowledged by the vendor or author of the affected technology. The vulnerability may also be Confirmed when its existence is confirmed from an external event such as publication of functional or proof-of-concept exploit code or widespread exploitation.
- **Not Defined (ND)** Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Environmental Metrics

Different environments can have an immense bearing on the risk that a vulnerability poses to an organization and its stakeholders. The CVSS environmental metric group captures the characteristics of a vulnerability that are associated with a user's IT environment. Since environmental metrics are optional they each include a metric value that has no effect on the score. This value is used when the user feels the particular metric does not apply and wishes to "skip over" it.

Collateral Damage Potential (CDP)

This metric measures the potential for loss of life or physical assets through damage or theft of property or equipment. The metric may also measure economic loss of productivity or revenue. The possible values for this metric are listed below. Naturally, the greater the damage potential, the higher the vulnerability score.

- **None (N)** There is no potential for loss of life, physical assets, productivity or revenue.

- **Low (L)** A successful exploit of this vulnerability may result in slight physical or property damage. Or, there may be a slight loss of revenue or productivity to the organization.
- **Low-Medium (LM)** A successful exploit of this vulnerability may result in moderate physical or property damage. Or, there may be a moderate loss of revenue or productivity to the organization.
- **Medium-High (MH)** A successful exploit of this vulnerability may result in significant physical or property damage or loss. Or, there may be a significant loss of revenue or productivity.
- **High (H)** A successful exploit of this vulnerability may result in catastrophic physical or property damage and loss. Or, there may be a catastrophic loss of revenue or productivity.
- **Not Defined (ND)** Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Clearly, each organization must determine for themselves the precise meaning of "slight, moderate, significant, and catastrophic."

Target Distribution (TD)

This metric measures the proportion of vulnerable systems. It is meant as an environment-specific indicator in order to approximate the percentage of systems that could be affected by the vulnerability. The possible values for this metric are listed below. The greater the proportion of vulnerable systems, the higher the score.

- **None (N)** No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting. Effectively 0% of the environment is at risk.
- **Low (L)** Targets exist inside the environment, but on a small scale. Between 1% - 25% of the total environment is at risk.
- **Medium (M)** Targets exist inside the environment, but on a medium scale. Between 26% - 75% of the total environment is at risk.
- **High (H)** Targets exist inside the environment on a considerable scale. Between 76% - 100% of the total environment is considered at risk.
- **Not Defined (ND)** Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Security Requirements (CR, IR, AR)

These metrics enable the analyst to customize the CVSS score depending on the importance of the affected IT asset to a users organization, measured in terms of confidentiality, integrity, and availability, That is, if an IT asset supports a business function for which availability is most important, the analyst can assign a greater value to availability, relative to confidentiality and integrity. Each security requirement has three possible values: low, medium, or high.

The full effect on the environmental score is determined by the corresponding base impact metrics (please note that the base confidentiality, integrity and availability impact metrics, themselves, are not changed). That is, these metrics modify the environmental score by reweighting

the (base) confidentiality, integrity, and availability impact metrics. For example, the confidentiality impact (C) metric has increased weight if the confidentiality requirement (CR) is high. Likewise, the confidentiality impact metric has decreased weight if the confidentiality requirement is low. The confidentiality impact metric weighting is neutral if the confidentiality requirement is medium. This same logic is applied to the integrity and availability requirements.

Note that the confidentiality requirement will not affect the environmental score if the (base) confidentiality impact is set to none. Also, increasing the confidentiality requirement from medium to high will not change the environmental score when the (base) impact metrics are set to complete. This is because the impact sub score (part of the base score that calculates impact) is already at a maximum value of 10.

The possible values for the security requirements are listed below. For brevity, the same table is used for all three metrics. The greater the security requirement, the higher the score (remember that medium is considered the default). These metrics will modify the score as much as plus or minus 2.5.

- **Low (L)** Loss of [confidentiality / integrity / availability] is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
- **Medium (M)** Loss of [confidentiality / integrity / availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
- **High (H)** Loss of [confidentiality / integrity / availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
- **Not Defined (ND)** Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.